AMENDMENTS TO THE SPECIFICATION

Please amend paragraphs [0037] and [0061] as follows.

[0037] Handshake protocol 302 enables endpoint A 102 (also referred to as "the client") and endpoint B 108 (also referred to as "the server") to communicate their need to register with each other. They may also communicate that they are capable of registering others as well. Thus, handshake protocol 302 is a bilateral protocol that enables endpoint A 102 to register endpoint B 108 and endpoint B 108 to register endpoint A 102. Handshake protocol 302 comprises a client hello message 304, a register_client_platform_request_pdu 308, a server hello message 310, a certificate 314, a server-key exchange message 316, a certificate request 318, a register_client_platform_response_pdu 320, a register_server_platform_request_pdu 322, a server hello done message 324, a certificate 326, a client-key exchange message 328, a certificate verify 330, an acknowledge_client_registration_pdu 332, a register_server_platform_response_pdu 334, a client change cipher spec message 336, a client finished message 338, an acknowledge_server_registration_pdu 340, a server change cipher spec message 342, and a server finished message 344. Each of the above-listed pdus (protocol data units) is an attestation protocol data unit according to embodiments of the present invention. The handshake structures for the pdus are based on the TLS Extensions, RFC 3546, ~~http://www.ietf.org/rfc/rfc3546.txt,~~ **currently available at www--ietf--org/rfc/rfc3546.txt, where the periods in the URL have been replaced with "--" to avoid inadvertent hyperlinking,** dated Jun. 2003. The remaining messages are TLS protocol messages as defined in The TLS Protocol Version 1.0, RFC 2246, ~~http://www.ietf.org/rfc/rfc2246.txt,~~ **currently available at www--ietf--org/rfc/rfc2246.txt, where the periods in the URL have been replaced with "--" to avoid inadvertent hyperlinking,** dated Jan. 1999.

[0061] Diagram 400 comprises endpoint A 102 communicating with endpoint B 108 through a bi-directional platform authentication and attestation handshake protocol 402. As indicated above with reference to FIG. 3A, handshake protocol 402 is described with endpoint A 102 acting as the client and endpoint B 108 acting as the server. Although the protocol is described as a client/server implementation, peer-to-peer implementations may also be used. Handshake protocol 402 comprises client hello message 304, a server_config_request_pdu 406,

server hello message 310, certificate 314, server-key exchange 316, certificate request 318, a server_credential_pdu 410, a server_platform_auth_pdu 412, a server_config_response_pdu 414, a client_config_request_pdu 416, server hello done message 324, certificate 326, a client_credential_pdu 418, a client_platform_auth_pdu 420, client-key exchange message 328, certificate verify 330, a client_config_response_pdu 422, change cipher spec 336, finished message 338, change cipher spec message 342, and finished message 344. As previously indicated, each of the above-listed pdus (protocol data units) is an attestation protocol data unit according to embodiments of the present invention. The handshake structures for the pdus are based on the TLS Extensions, RFC 3546, ~~**http://www.ietf.org/rfc/rfc3546.txt,**~~ **currently available at www--ietf--org/rfc/rfc3546.txt, where the periods in the URL have been replaced with "--" to avoid inadvertent hyperlinking,** dated Jun. 2003. The remaining messages are TLS protocol messages as defined in The TLS Protocol Version 1.0, RFC 2246, ~~**http://www.ietf.org/rfc/rfc2246.txt,**~~ **currently available at www--ietf--org/rfc/rfc2246.txt, where the periods in the URL have been replaced with "--" to avoid inadvertent hyperlinking,** dated Jan. 1999.